ELECTRONIC PEN, AND SYSTEM AND METHOD FOR INDIVIDUAL AUTHENTICATION

Patent number:	JP10222241
Publication date:	1998-08-21
Inventor:	OKAZAKI MASARU
Applicant:	CANON INC
Classification:	
- international:	G06F1/00; G06F3/033; G06F12/14; G06T7/00
- european:	
Application number:	JP19970035646 19970204
Priority number(s):	

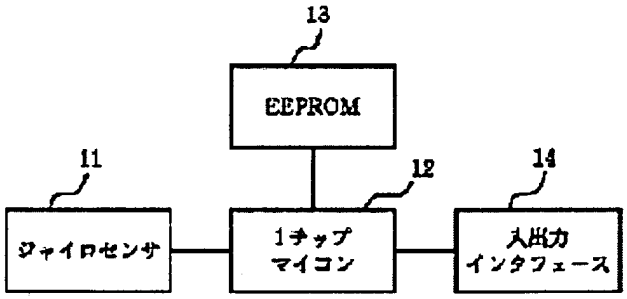
Also published as:

JP10222241 (A)

Abstract of **JP10222241**

PROBLEM TO BE SOLVED: To accurately authenticate an individual by a simple method which saves trouble and to completely obtain the security of a computer by authenticating the individual through comparison between stored signature feature data and an electronic pen signature result.

SOLUTION: An electronic pen has a gyro sensor 11, a one-chip microcomputer 12, an EEPROM 13, and an input/output interface 14 inside. The one-chip microcomputer 12 authenticates an individual according to features of the track and stroke speed of the electronic pen and has algorithm for generating a unique password according to the previously stored characteristic number and features of strokes of the electronic pen. The EEPROM 13 is an electrically erasable read-only memory and stored with user's signature feature data. The one-chip microcomputer 12 authenticates the individual through comparison between the signature feature data and the features of the track and stroke speed of the electronic pen.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－222241

(43)公開日　平成10年(1998)８月21日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	1/00	３７０	Ｇ０６Ｆ	1/00	３７０Ｅ
	3/033	３２０		3/033	３２０
	12/14	３２０		12/14	３２０Ｃ
Ｇ０６Ｔ	7/00			15/62	４６５Ｐ

審査請求　未請求　請求項の数20　ＦＤ　（全９頁）

(21)出願番号　特願平9－35646

(22)出願日　平成９年(1997)２月４日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　岡▲崎▼　大
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

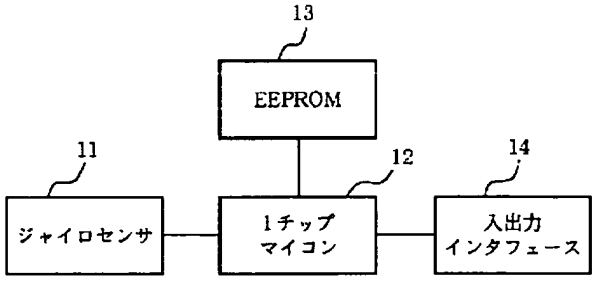
(74)代理人　弁理士　渡部　敏彦

(54)【発明の名称】　電子ペン及び個人認証システム並びに個人認証方法

(57)【要約】

【課題】　手間をかけない簡単な方法により、個人認証を的確に行ってコンピュータのセキュリティを万全に確保すること等を可能とした電子ペン及び個人認証システム並びに個人認証方法を提供する。

【解決手段】　電子ペンは、ユーザの署名の特徴データを記憶したＥＥＰＲＯＭ１３と、空間における電子ペンの相対位置を検出するジャイロセンサ１１と、電子ペンを使用して空間で署名した個人の署名がＥＥＰＲＯＭ１３に予め記憶されている署名の特徴データを有する持ち主と同一人物か否かの判定に基づき個人認証を行うと共に、電子ペンの固有番号と署名の特徴とに基づきパスワードを作成するワンチップマイクロコンピュータ１２とを具備する。



【特許請求の範囲】
【請求項1】　コンピュータ入力装置として使用され署名を行った個人を認証する電子ペンであって、
所定の署名特徴データを記憶した署名特徴記憶手段と、前記署名特徴データと電子ペン署名結果との比較に基づき個人を認証する認証手段とを具備することを特徴とする電子ペン。
【請求項2】　請求項1記載の電子ペンにおいて、電子ペン固有番号を記憶した固有番号記憶手段を具備すると共に、前記署名特徴記憶手段は再記録が可能であることを特徴とする電子ペン。
【請求項3】　請求項1又は2記載の電子ペンにおいて、空間で署名を行うことを特徴とする電子ペン。
【請求項4】　請求項1、2又は3記載の電子ペンにおいて、前記認証手段は、前記署名特徴データと空間での署名に伴う電子ペン軌跡及び筆速の特徴との比較に基づき個人を認証することを特徴とする電子ペン。
【請求項5】　請求項1、2、3又は4記載の電子ペンにおいて、空間での署名に伴う電子ペン相対位置を検出する位置検出手段を具備することを特徴とする電子ペン。
【請求項6】　請求項1、2、3、4又は5記載の電子ペンにおいて、前記電子ペン固有番号と空間での署名に伴う電子ペン軌跡及び筆速の特徴とに基づきパスワードを作成するパスワード作成手段を具備することを特徴とする電子ペン。
【請求項7】　請求項6記載の電子ペンにおいて、前記パスワード作成手段は、前記認証手段が個人認証を行うことができなかった場合は偽のパスワードを作成することを特徴とする電子ペン。
【請求項8】　請求項6又は7記載の電子ペンにおいて、前記パスワードは、文字情報ではなく適度に長いバイナリ列であることを特徴とする電子ペン。
【請求項9】　請求項6、7又は8記載の電子ペンにおいて、前記電子ペン固有番号及びパスワードからなるセキュリティ情報をコンピュータへ伝達する伝達手段を具備することを特徴とする電子ペン。
【請求項10】　請求項9記載の電子ペンにおいて、前記セキュリティ情報は、電気信号、光、振動等の何れかにより伝達されることを特徴とする電子ペン。
【請求項11】　請求項1、2、3、4、5、6、7、8、9又は10記載の電子ペンとコンピュータとを具備してなり、該電子ペン及びコンピュータによりコンピュータ使用を所望する個人を認証することを特徴とする個人認証システム。
【請求項12】　コンピュータ入力装置として使用され署名を行った個人を認証する電子ペンを用いて個人の認証を行う個人認証方法であって、
予め設定された所定の署名特徴データと電子ペン署名結果との比較に基づき個人を認証する認証ステップを有することを特徴とする個人認証方法。
【請求項13】　請求項12記載の個人認証方法において、前記電子ペンにより空間で署名を行うことを特徴とする個人認証方法。
【請求項14】　請求項12又は13記載の個人認証方法において、前記認証ステップでは、前記署名特徴データと空間での署名に伴う電子ペン軌跡及び筆速の特徴との比較に基づき個人を認証することを特徴とする個人認証方法。
【請求項15】　請求項12、13又は14記載の個人認証方法において、空間での署名に伴う電子ペン相対位置を検出する位置検出ステップを有することを特徴とする個人認証方法。
【請求項16】　請求項12、13、14又は15記載の個人認証方法において、電子ペンに予め記憶された電子ペン固有番号と空間での署名に伴う電子ペン軌跡及び筆速の特徴とに基づきパスワードを作成するパスワード作成ステップを有することを特徴とする個人認証方法。
【請求項17】　請求項16記載の個人認証方法において、前記パスワード作成ステップでは、前記認証ステップで個人認証を行うことができなかった場合は偽のパスワードを作成することを特徴とする個人認証方法。
【請求項18】　請求項16又は17記載の個人認証方法において、前記パスワードは、文字情報ではなく適度に長いバイナリ列であることを特徴とする個人認証方法。
【請求項19】　請求項16、17又は18記載の個人認証方法において、前記電子ペン固有番号及びパスワードからなるセキュリティ情報をコンピュータへ伝達する伝達ステップを有することを特徴とする個人認証方法。
【請求項20】　請求項19記載の個人認証方法において、前記セキュリティ情報は、電気信号、光、振動等の何れかにより伝達されることを特徴とする個人認証方法。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、電子ペン及び個人認証システム並びに個人認証方法に係り、更に詳しくは、セキュリティを万全に確保すると共に個人認証を的確に行う場合等に好適な電子ペン及び個人認証システム並びに個人認証方法に関する。
【0002】
【従来の技術】従来、個人を認証する方法としては、個人識別を必要とするセキュリティ対象となるコンピュータのＯＳ（Operating System）のように、本人周囲の人間など誰でも知っている個人を示す名称と、本人しか知らないパスワードとを照合することにより個人認証を行う方法、或いは、キャッシュカードのように、カードの番号とパスワードをサーバ（外部から受けた要求を処理するコンピュータまたはプログラム）側が予め記憶し

ておき、外部から打ち込まれたカード番号とパスワードを照合することにより個人認証を行う方法、或いは、本人が署名したサインを照合することにより個人認証を行う方法等、各種の個人認証方法がある。

【０００３】図６は従来例に係る個人認証システムの構成を示す図であり、本人が署名したサインを照合して個人認証を行うシステムである。該個人認証システムは、コンピュータ８４と、該コンピュータ８４に接続されたパッド８１と、ペン８３とを備える構成となっている。

【０００４】上記各部の構成を説明すると、コンピュータ８４は、セキュリティの対象となるコンピュータであり、予め筆跡データベースを記憶している。パッド８１には、ペン８３を用いて書かれた筆跡を認証する筆跡認証エリア８２が配設されており、上からの圧力を検出する素子が所定の定められた細かいドットピッチで張り巡らされており、ペン８３の先端が接触している座標、圧力を逐次検出することにより、筆跡及び筆圧を検出する機能を有する。ペン８３は、パッド８１の筆跡認証エリア８２内に対するサインの署名に使用される。

【０００５】コンピュータ８４におけるセキュリティの必要な操作を行う場合には、ユーザはペン８３を用いて、パッド８１の筆跡認証エリア８２内にサイン（signature）を書く。サインの署名に伴い、パッド８１は、筆跡認証エリア８２に接触しているペン８３の先端の座標、圧力を逐次検出することにより筆跡及び筆圧を検出し、コンピュータ８４へ転送する。これにより、コンピュータ８４は、予め記憶してある筆跡データベースに基づき、パッド８１及びペン８３を介して入力されたサインの署名者がコンピュータ８４を使用して作業を行ってもよいか否かを判別する。

【０００６】

【発明が解決しようとする課題】しかしながら、上述した従来技術においては下記のような問題があった。即ち、上記図６に示したような個人認証システムを用いた個人認証方式では、一度、ログイン（データの送受やファイル操作が可能となる状態）してしまうと、セキュリティ対象のコンピュータ８４をそのまま使用することができるため、ユーザがコンピュータ８４の周囲から席を外す場合には、セキュリティを犠牲にしてコンピュータ８４を立ち上げたままの状態で席を立つか、或いは、面倒でもログアウト（接続を切り終了した状態）してから席を立つしかないという問題があった。

【０００７】本発明は、上述した点に鑑みなされたものであり、手間をかけない簡単な方法により、個人認証を的確に行ってコンピュータのセキュリティを万全に確保すること等を可能とした電子ペン及び個人認証システム並びに個人認証方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】上記目的を達成するため、請求項１の発明は、コンピュータ入力装置として使用され署名を行った個人を認証する電子ペンであって、所定の署名特徴データを記憶した署名特徴記憶手段と、前記署名特徴データと電子ペン署名結果との比較に基づき個人を認証する認証手段を具備することを特徴とする。

【０００９】上記目的を達成するため、請求項２の発明は、請求項１記載の電子ペンにおいて、電子ペン固有番号を記憶した固有番号記憶手段を具備すると共に、前記署名特徴記憶手段は再記録が可能であることを特徴とする。

【００１０】上記目的を達成するため、請求項３の発明は、請求項１又は２記載の電子ペンにおいて、空間で署名を行うことを特徴とする。

【００１１】上記目的を達成するため、請求項４の発明は、請求項１、２又は３記載の電子ペンにおいて、前記認証手段は、前記署名特徴データと空間での署名に伴う電子ペン軌跡及び筆速の特徴との比較に基づき個人を認証することを特徴とする。

【００１２】上記目的を達成するため、請求項５の発明は、請求項１、２、３又は４記載の電子ペンにおいて、空間での署名に伴う電子ペン相対位置を検出する位置検出手段を具備することを特徴とする。

【００１３】上記目的を達成するため、請求項６の発明は、請求項１、２、３、４又は５記載の電子ペンにおいて、前記電子ペン固有番号と空間での署名に伴う電子ペン軌跡及び筆速の特徴とに基づきパスワードを作成するパスワード作成手段を具備することを特徴とする。

【００１４】上記目的を達成するため、請求項７の発明は、請求項６記載の電子ペンにおいて、前記パスワード作成手段は、前記認証手段が個人認証を行うことができなかった場合は偽のパスワードを作成することを特徴とする。

【００１５】上記目的を達成するため、請求項８の発明は、請求項６又は７記載の電子ペンにおいて、前記パスワードは、文字情報ではなく適度に長いバイナリ列であることを特徴とする。

【００１６】上記目的を達成するため、請求項９の発明は、請求項６、７又は８記載の電子ペンにおいて、前記電子ペン固有番号及びパスワードからなるセキュリティ情報をコンピュータへ伝達する伝達手段を具備することを特徴とする。

【００１７】上記目的を達成するため、請求項１０の発明は、請求項９記載の電子ペンにおいて、前記セキュリティ情報は、電気信号、光、振動等の何れかにより伝達されることを特徴とする。

【００１８】上記目的を達成するため、請求項１１の発明は、請求項１、２、３、４、５、６、７、８、９又は１０記載の電子ペンとコンピュータとを具備してなり、該電子ペン及びコンピュータによりコンピュータ使用を所望する個人を認証することを特徴とする。

【００１９】上記目的を達成するため、請求項１２の発明は、コンピュータ入力装置として使用され署名を行った個人を認証する電子ペンを用いて個人の認証を行う個人認証方法であって、予め設定された所定の署名特徴データと電子ペン署名結果との比較に基づき個人を認証する認証ステップを有することを特徴とする。

【００２０】上記目的を達成するため、請求項１３の発明は、請求項１２記載の個人認証方法において、前記電子ペンにより空間で署名を行うことを特徴とする。

【００２１】上記目的を達成するため、請求項１４の発明は、請求項１２又は１３記載の個人認証方法において、前記認証ステップでは、前記署名特徴データと空間での署名に伴う電子ペン軌跡及び筆速の特徴との比較に基づき個人を認証することを特徴とする。

【００２２】上記目的を達成するため、請求項１５の発明は、請求項１２、１３又は１４記載の個人認証方法において、空間での署名に伴う電子ペン相対位置を検出する位置検出ステップを有することを特徴とする。

【００２３】上記目的を達成するため、請求項１６の発明は、請求項１２、１３、１４又は１５記載の個人認証方法において、電子ペンに予め記憶された電子ペン固有番号と空間での署名に伴う電子ペン軌跡及び筆速の特徴とに基づきパスワードを作成するパスワード作成ステップを有することを特徴とする。

【００２４】上記目的を達成するため、請求項１７の発明は、請求項１６記載の個人認証方法において、前記パスワード作成ステップでは、前記認証ステップで個人認証を行うことができなかった場合は偽のパスワードを作成することを特徴とする。

【００２５】上記目的を達成するため、請求項１８の発明は、請求項１６又は１７記載の個人認証方法において、前記パスワードは、文字情報ではなく適度に長いバイナリ列であることを特徴とする。

【００２６】上記目的を達成するため、請求項１９の発明は、請求項１６、１７又は１８記載の個人認証方法において、前記電子ペン固有番号及びパスワードからなるセキュリティ情報をコンピュータへ伝達する伝達ステップを有することを特徴とする。

【００２７】上記目的を達成するため、請求項２０の発明は、請求項１９記載の個人認証方法において、前記セキュリティ情報は、電気信号、光、振動等の何れかにより伝達されることを特徴とする。

【００２８】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。

【００２９】先ず、本実施の形態に係る電子ペンの構成を図１を参照して説明する。図１は電子ペンの電気的構成を示すブロック図である。電子ペンは、ジャイロセンサ１１と、ワンチップマイクロコンピュータ（以下、ワンチップマイコンと略称）１２と、ＥＥＰＲＯＭ（Electrically Erasable Programmable Read Only Memory）１３と、入出力インタフェース１４とを電子ペン内部に備えた構成となっている。

【００３０】上記各部の構成を詳述すると、ジャイロセンサ１１は、電子ペン内部に装備するために小型化されており、空間における電子ペンの相対位置を検出するセンサである。ワンチップマイコン１２は、後述する図２のフローチャートのステップＳ２乃至ステップＳ４に示される処理を行うと共に電子ペン各部の制御を行うものであり、電子ペンの軌跡及び筆速の特徴に基づき個人を検証し、予め記憶してある電子ペンの固有番号（ＩＤ）及び筆跡の特徴に基づき独特のパスワードを生成するアルゴリズムを有している。尚、電子ペンが個人の認証に失敗した場合には、パスワード作成時に偽のパスワードが作成される。

【００３１】ＥＥＰＲＯＭ１３は、電気的消去が可能な読み出し専用メモリであり、ユーザ情報（ユーザの署名の特徴に関する情報）が記憶されている。入出力インタフェース１４は、電子ペン内部の処理した結果とコンピュータ（図示略）側の情報とを互いに通信するための手段であり、電子ペンの固有番号及びパスワードからなるセキュリティ情報をコンピュータへ送信する機能を有している。尚、セキュリティ情報は、電気信号もしくは光もしくは振動によりコンピュータへ伝達することが可能である。

【００３２】次に、本実施の形態に係る電子ペンの外観及びコンピュータ側のソケットに対する電子ペンの挿入状態について図３（ａ）、（ｂ）を参照して説明する。図３（ａ）は電子ペンの外観図、図３（ｂ）はコンピュータ側のソケットに電子ペンを挿入した状態を示す一部を断面とした説明図である。電子ペンは、筐体３１にファンクションスイッチ３２と電極３３とを装備している。また、コンピュータ側には、該コンピュータと電子ペンと間における情報をやり取りするための電極（図示略）を有するソケット３４が装備されている。

【００３３】次に、本実施の形態に係る電子ペンを使用して個人認証を行う場合の動作の流れについて図２のフローチャートを参照して説明する。図２のフローチャートでは、ステップＳ２乃至ステップＳ４の処理を電子ペン側で行い、ステップＳ５及びステップＳ６の処理をコンピュータ側で行う。この場合、電子ペンのＥＥＰＲＯＭ１３には、既にユーザの署名の特徴が抽出されて保存されているものと仮定する。

【００３４】図２において、先ず、ユーザは自分自身を電子ペンに認証させるに際して、図４（ａ）に示すごとく普通にペンを持つのと同様に電子ペンを持ち、空間の一部（署名を書き始める場所）まで手を移動させ、電子ペンのファンクションスイッチ３２を指で押さえながら、図４（ｂ）に示すごとく空間で署名を描く（ステップＳ１）。ユーザがファンクションスイッチ３２を押さ

えている間、電子ペンのジャイロセンサ１１は空間における電子ペンの相対位置を計測し続け、一定時間間隔でサンプリングし、サンプリング結果をワンチップマイコン１２へ入力する（ステップＳ２）。

【００３５】ユーザは電子ペンを使用して署名を書き終わったならば、直ちに電子ペンのファンクションスイッチ３２から指を離す。これに伴い、電子ペンのワンチップマイコン１２はユーザによる電子ペンを使用した署名の入力が終了したと認識し、予め設定されているサインデータベース（signature data base）に基づき署名の検証を開始する（ステップＳ３）。

【００３６】ところで、署名の検証方法は数多く存在するが、本実施の形態では以下に示す方法で説明する。図５（ａ）は署名を検証するための元となる署名を示す図であり、署名を検証するための元となる署名のデータは電子ペンのＥＥＰＲＯＭ１３に保存されている。図５（ｂ）はユーザがログインするために電子ペンで入力した署名を示す図である。

【００３７】図５（ａ）、（ｂ）には各々座標が記入されているが、これは順番にＸ、Ｙ、Ｚ（ｘ、ｙ、ｚ）の空間座標と時間Ｔ（ｔ）を表している。また、図５（ａ）の点Ｐ１～Ｐ６、図５（ｂ）の点ｐ１～ｐ６は、各々空間座標Ｘ、Ｙ、Ｚ軸、ｘ、ｙ、ｚ軸において向きの正負が入れ替わる点である。これら各点の距離間隔の比が略正しく、且つ、時間間隔比が略一致した場合は、予め用意された署名の持ち主と、新たに電子ペンを使用して署名した人物とが、同一人物であると判定する。即ち、

【００３８】

【数１】

$$\overline{O,P1}:\overline{P1,P2}:\overline{P2,P3}:\ldots:\overline{P5,P6} \fallingdotseq \overline{O,p1}:\overline{p1,p2}:\overline{p2,p3}:\ldots:\overline{p5,p6}$$

$$T1-T0:T2-T1:T3-T2:\ldots:T6-T5 \fallingdotseq t1-t0:t2-t1:t3-t2:\ldots:t6-t5$$

で表される式が成立すれば、同一人物であると判定する。上述した署名検証方法によりユーザ判定が終了すると、再度図２において、電子ペンのワンチップマイコン１２は電子ペンの固有番号と署名の特徴に基づき、パスワードを作成する（ステップＳ４）。

【００３９】ここで、パスワードの作成には、署名を検証するときに参照する特徴点０、Ｐ１、Ｐ２、Ｐ３、Ｐ４、Ｐ５、Ｐ６のうち、Ｐ１、Ｐ２、Ｐ３、Ｐ４、Ｐ５、即ち、Ｐに付属する番号のうち、３の倍数を取り除いた点を用いる。また、電子ペンの固有番号をαとする。それぞれの点Ｐ１、Ｐ２、・・・に対し、

【００４０】

【数２】

$$\beta 1 = (x1 + y1 + z1) \,\&\, \alpha \qquad \beta 2 = (x2 + y2 + z2) \,\&\, \alpha$$

$$\beta 4 = (x4 + y4 + z4) \,\&\, \alpha \qquad \beta 5 = (x5 + y5 + z5) \,\&\, \alpha$$

で表される式に基づき、β１、β２、β４、β５を決定する。β１、β２、β４、β５は、それぞれ電子ペンの固有番号αと同一の長さのバイナリ列である。パスワードは、上記β１、β２、β４、β５のバイナリ列を並べただけのものとする。即ち、このバイナリ長は、$\alpha \times 4$となる。仮に、ユーザの署名の入力で、電子ペンの使用が許可されなかった場合には、値、長さ共にランダムなバイナリ列を作る。

【００４１】次に、上記電子ペンで作成したパスワード及び電子ペンをコンピュータに認識させて署名ユーザの判別を行うべく、ユーザは電子ペンの筐体３１をコンピュータ側に予め装備されているソケット３４に挿入する（上記図３（ｂ）参照）。

【００４２】再度図２において、電子ペンの筐体３１の電極３３とコンピュータ側のソケット３４の電極（図示略）との接触に伴い、電気的な通信路が確保されたならば、電子ペンは直ちに電子ペンの固有番号α、そして、固有番号αに続いてパスワードをそのままコンピュータ側へ転送する。コンピュータは電子ペンの固有の番号αとパスワードとを用いて、電子ペンがユーザの使用を許可したか否かの検証を行う（ステップＳ５）。

【００４３】即ち、コンピュータはパスワードを電子ペンの固有番号αの長さに分割して、β１、β２、β４、β５を再構築する。この時点でうまく分割できなかった場合は、ユーザのコンピュータに対するログインを許可しない（ステップＳ６）。次に、β１、β２、β４、β５を電子ペンの固有番号αとＯＲ（論理和）を取り、結果がαにならない場合は、ユーザのコンピュータに対するログインを許可しない（ステップＳ６）。更に、コンピュータがログイン許可テーブルを装備していれば、該テーブルの参照に基づき、許可されたユーザの電子ペンの固有番号である場合は、ユーザのコンピュータに対するログインを許可する（ステップＳ６）。

【００４４】上述したように、本実施の形態によれば、電子ペンは、所定の署名特徴データを記憶したＥＥＰＲＯＭ１３と、前記署名特徴データと電子ペンの軌跡及び筆速の特徴との比較に基づき個人を認証するワンチップマイコン１２とを具備しているため、電子ペンで署名した個人が予め登録されたコンピュータ使用許可者であるか否かを的確に認証することができ、これにより、セキュリティを確保することができる。

【００４５】また、電子ペンは、予め固有番号を有すると共に、ＥＥＰＲＯＭ１３は再記録が可能であるため、固有番号を有する電子ペンにより予め登録されている署

名を行ったユーザしかコンピュータを使用することができないと共に、ユーザの特徴に応じた情報を電子ペンに記録しておくことができ、これにより、セキュリティを確保することができる。

【００４６】また、電子ペンは、空間での署名に伴う電子ペン相対位置を検出するジャイロセンサ１１を具備しているため、従来のごとく電子ペンの筆跡や筆圧を検出するための署名入力用パッドが不要となる。

【００４７】また、電子ペンは、電子ペンの固有番号と空間での署名に伴う電子ペンの軌跡及び筆速の特徴とに基づきパスワードを作成するパスワード作成アルゴリズムを有しているため、コンピュータ入力装置としての電子ペンの側でセキュリティチェックを万全に施すことができる。

【００４８】また、電子ペンは、電子ペンで個人認証を行うことができなかった場合は偽のパスワードを上記パスワード作成アルゴリズムにより作成するため、コンピュータ側に対してコンピュータ使用許可者以外の者が電子ペンを使用した旨を警告することができる。

【００４９】また、電子ペンは、文字情報ではなく適度に長いバイナリ列からなるパスワードを作成するため、該バイナリ列を人間が覚えることができないくらいの長さに設定しておけば、コンピュータ使用許可者以外の者が模写することは困難となり、これにより、セキュリティを万全に確保することができる。

【００５０】また、電子ペンは、固有番号及びパスワードからなるセキュリティ情報をコンピュータへ伝達する入出力インタフェース１４を具備しているため、コンピュータ側にユーザを識別させることができる。

【００５１】また、電子ペンは、上記セキュリティ情報を電気信号、光、振動等の何れかにより伝達することが可能であるため、上記と同様にコンピュータ側にユーザを識別させることができる。

【００５２】従って、上述した点から、ユーザがコンピュータシステムを運用するに際しては、電子ペンとコンピュータとの両方で二重にセキュリティガードをかけることができ、これにより、セキュリティを万全に確保することができる。

【００５３】また、ユーザがコンピュータの前から席を外すときに、或る一定時間以内に電子ペンからの入力がない場合は、電子ペンからの固有番号及びパスワードを再度受け付けなければ再度入力ができないようにシステムを構成すれば、ユーザが席を一定時間以上離れるときに電子ペンを所持して行けば、他人がコンピュータを操作することはできなくなる。

【００５４】この場合、電子ペン側は一度ログインを受け付けているので、ユーザは再度署名を書く必要はなく、コンピュータ側のソケットに電子ペンを再度挿入すれば、電子ペンは電子ペンの固有番号とパスワードをコンピュータ側に再度送信し、コンピュータ側がこれを検証することにより、コンピュータの再操作が可能となる。

【００５５】また、パスワードは電子ペン側で作成するものの、パスワードはバイナリの長い列で且つユーザの署名の特徴のうちの全てを用いないようにすることにより、他人がパスワードを破ることは困難となる。他方、署名をパスワードに用いることにより、ユーザ側はパスワードを覚える必要がなくなるため、パスワードを覚える煩雑さやパスワードを忘失したりする不具合を解消することができる。

【００５６】尚、本発明は、複数の機器から構成されるシステムに適用しても、１つの機器からなる装置に適用してもよい。前述した実施形態の機能を実現するソフトウエアのプログラムコードを記憶した記憶媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。

【００５７】この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【００５８】プログラムコードを供給するための記憶媒体としては、例えば、フロッピディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどを用いることができる。

【００５９】また、コンピュータが読出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているＯＳなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００６０】更に、記憶媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００６１】

【発明の効果】以上説明したように、請求項１の発明によれば、コンピュータ入力装置として使用され署名を行った個人を認証する電子ペンであって、所定の署名特徴データを記憶した署名特徴記憶手段と、前記署名特徴データと電子ペン署名結果との比較に基づき個人を認証する認証手段とを具備しているため、電子ペンで署名した個人が予め登録されたコンピュータ使用許可者であるか

否かを的確に認証することができ、これにより、セキュリティを確保することができる。

【0062】請求項2の発明によれば、請求項1記載の電子ペンにおいて、電子ペン固有番号を記憶した固有番号記憶手段を具備すると共に、前記署名特徴記憶手段は再記録が可能であるため、固有番号を有する電子ペンにより予め登録されている署名を行ったユーザしかコンピュータを使用することができないと共に、ユーザの特徴に応じた情報を電子ペンに記録しておくことができ、これにより、セキュリティを確保することができる。

【0063】請求項3の発明によれば、請求項1又は2記載の電子ペンにおいて、空間で電子ペンによる署名を行うため、従来のごとく電子ペンの筆跡や筆圧を検出するための署名入力用パッドが不要となる。

【0064】請求項4の発明によれば、請求項1、2又は3記載の電子ペンにおいて、前記認証手段は、前記署名特徴データと空間での署名に伴う電子ペン軌跡及び筆速の特徴との比較に基づき個人を認証するため、請求項1の発明と同様に、電子ペンで署名した個人が予め登録されたコンピュータ使用許可者であるか否かを的確に認証することができ、これにより、セキュリティを確保することができる。

【0065】請求項5の発明によれば、請求項1、2、3又は4記載の電子ペンにおいて、空間での署名に伴う電子ペン相対位置を検出する位置検出手段を具備しているため、従来のごとく電子ペンの筆跡や筆圧を検出するための署名入力用パッドが不要となる。

【0066】請求項6の発明によれば、請求項1、2、3、4又は5記載の電子ペンにおいて、前記電子ペン固有番号と空間での署名に伴う電子ペン軌跡及び筆速の特徴とに基づきパスワードを作成するパスワード作成手段を具備しているため、コンピュータ入力装置としての電子ペンの側でセキュリティチェックを万全に施すことができる。

【0067】請求項7の発明によれば、請求項6記載の電子ペンにおいて、前記パスワード作成手段は、前記認証手段が個人認証を行うことができなかった場合は偽のパスワードを作成するため、コンピュータ側に対してコンピュータ使用許可者以外の者が電子ペンを使用した旨を警告することができる。

【0068】請求項8の発明によれば、請求項6又は7記載の電子ペンにおいて、前記パスワードは、文字情報ではなく適度に長いバイナリ列であるため、該バイナリ列を人間が覚えることができないくらいの長さに設定しておけば、コンピュータ使用許可者以外の者が模写することは困難となり、これにより、セキュリティを万全に確保することができる。

【0069】請求項9の発明によれば、請求項6、7又は8記載の電子ペンにおいて、前記電子ペン固有番号及びパスワードからなるセキュリティ情報をコンピュータへ伝達する伝達手段を具備しているため、コンピュータ側にユーザを識別させることができる。

【0070】請求項10の発明によれば、請求項9記載の電子ペンにおいて、前記セキュリティ情報は、電気信号、光、振動等の何れかにより伝達されるため、請求項9の発明と同様に、コンピュータ側にユーザを識別させることができる。

【0071】請求項11の発明によれば、請求項1、2、3、4、5、6、7、8、9又は10記載の電子ペンとコンピュータとを具備してなり、該電子ペン及びコンピュータによりコンピュータ使用を所望する個人を認証するため、請求項1乃至請求項10の発明と同様の効果を奏することができる。

【0072】請求項12の発明によれば、コンピュータ入力装置として使用され署名を行った個人を認証する電子ペンを用いて個人の認証を行う個人認証方法であって、予め設定された所定の署名特徴データと電子ペン署名結果との比較に基づき個人を認証する認証ステップを有するため、電子ペンで署名した個人が予め登録されたコンピュータ使用許可者であるか否かを的確に認証することができ、これにより、セキュリティを確保することができる。

【0073】請求項13の発明によれば、請求項12記載の個人認証方法において、前記電子ペンにより空間で署名を行うため、従来のごとく電子ペンの筆跡や筆圧を検出するための署名入力用パッドが不要となる。

【0074】請求項14の発明によれば、請求項12又は13記載の個人認証方法において、前記認証ステップでは、前記署名特徴データと空間での署名に伴う電子ペン軌跡及び筆速の特徴との比較に基づき個人を認証するため、請求項12の発明と同様に、電子ペンで署名した個人が予め登録されたコンピュータ使用許可者であるか否かを的確に認証することができ、これにより、セキュリティを確保することができる。

【0075】請求項15の発明によれば、請求項12、13又は14記載の個人認証方法において、空間での署名に伴う電子ペン相対位置を検出する位置検出ステップを有するため、従来のごとく電子ペンの筆跡や筆圧を検出するための署名入力用パッドが不要となる。

【0076】請求項16の発明によれば、請求項12、13、14又は15記載の個人認証方法において、電子ペンに予め記憶された電子ペン固有番号と空間での署名に伴う電子ペン軌跡及び筆速の特徴とに基づきパスワードを作成するパスワード作成ステップを有するため、コンピュータ入力装置としての電子ペンの側でセキュリティチェックを万全に施すことができる。

【0077】請求項17の発明によれば、請求項16記載の個人認証方法において、前記パスワード作成ステップでは、前記認証ステップで個人認証を行うことができなかった場合は偽のパスワードを作成するため、コンピ

ュータ側に対してコンピュータ使用許可者以外の者が電子ペンを使用した旨を警告することができる。

【００７８】請求項１８の発明によれば、請求項１６又は１７記載の個人認証方法において、前記パスワードは、文字情報ではなく適度に長いバイナリ列であるため、該バイナリ列を人間が覚えることができないくらいの長さに設定しておけば、コンピュータ使用許可者以外の者が模写することは困難となり、これにより、セキュリティを万全に確保することができる。

【００７９】請求項１９の発明によれば、請求項１６、１７又は１８記載の個人認証方法において、前記電子ペン固有番号及びパスワードからなるセキュリティ情報をコンピュータへ伝達する伝達ステップを有するため、コンピュータ側にユーザを識別させることができる。

【００８０】請求項２０の発明によれば、請求項１９記載の個人認証方法において、前記セキュリティ情報は、電気信号、光、振動等の何れかにより伝達されるため、請求項１９の発明と同様に、コンピュータ側にユーザを識別させることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る電子ペンの電気的構成を示すブロック図である。

【図２】本発明の実施の形態に係る電子ペンを使用して個人認証を行う場合の動作の流れを示すフローチャートである。

【図３】本発明の実施の形態に係る電子ペン及びコンピュータ側に接続した電子ペンを示す図であり、（ａ）は電子ペンの外観図、（ｂ）はコンピュータ側のソケットに電子ペンを挿入した状態を示す一部を断面とした説明図である。

【図４】本発明の実施の形態に係る電子ペンで署名を行う状態を示す図であり、（ａ）はユーザが電子ペンを所持した状態を示す説明図、（ｂ）はユーザが所持した電子ペンにより空間で署名している状態を示す説明図である。

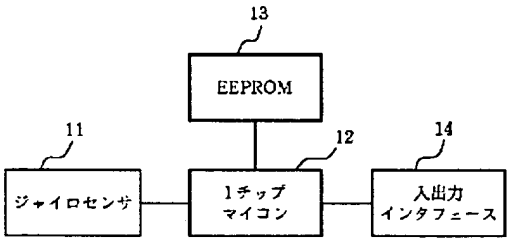
【図５】本発明の実施の形態に係る署名の座標を示す図であり、（ａ）は署名を検証するための元となる署名をＸＹ座標系に表した説明図、（ｂ）はユーザがログインするために電子ペンで入力した署名をＸＹ座標系に表した説明図である。

【図６】従来例に係る個人認証システムの構成を示す説明図である。

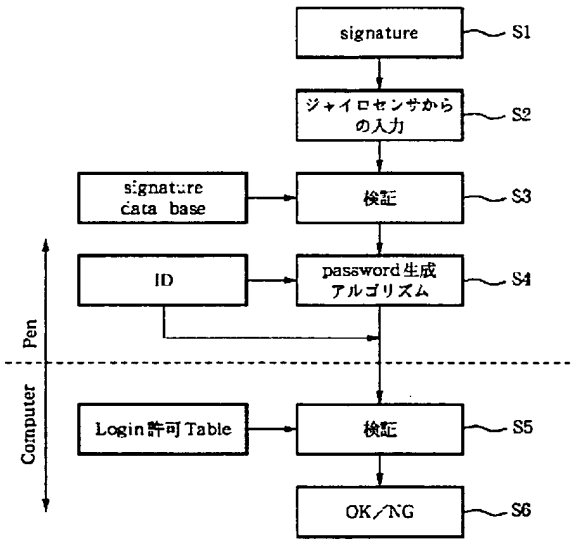
【符号の説明】

１１　ジャイロセンサ
１２　ワンチップマイクロコンピュータ
１３　ＥＥＰＲＯＭ
１４　入出力インタフェース
３１　筐体
３２　ファンクションスイッチ
３３　電極
３４　ソケット

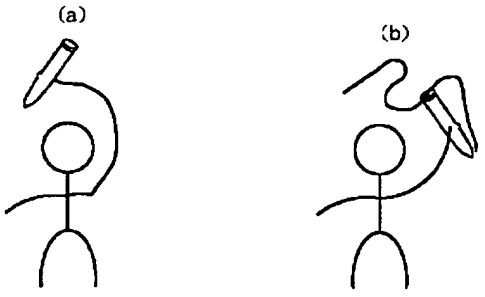
【図１】



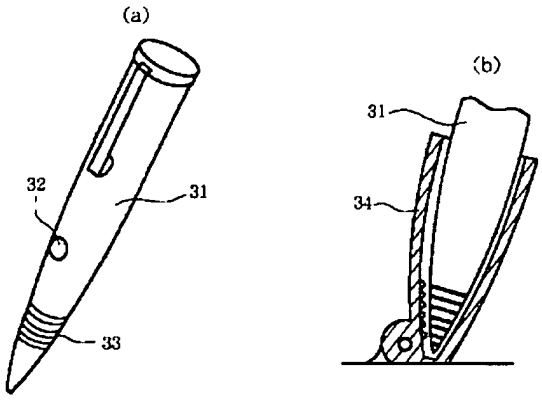
【図２】



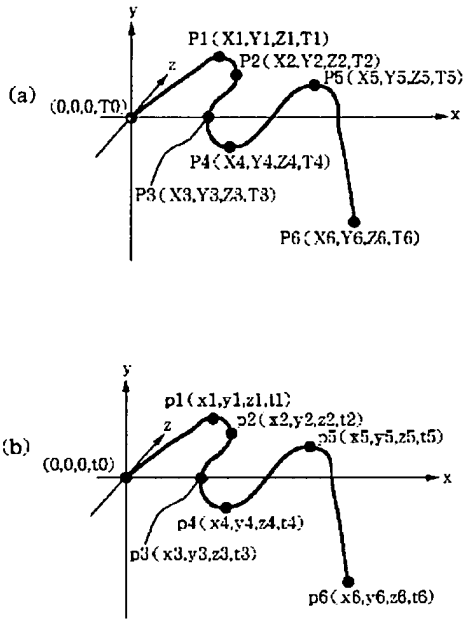
【図４】



【図3】



【図5】



【図6】